Release Notes for McAfee Endpoint Encryption for PC 6.1 Patch 3 with HF7409862

- About this document
- About this release
- EEPC 6.1 Patch 3 with HF7409862 features
- Requirements
- Known issues
- Resolved issues
- Documentation
- Supported Tokens and Readers
- Before installing EEPC 6.1 Patch 3 with HF7409862

About this document

Thank you for using McAfee Endpoint Encryption for PC 6.1 Patch 3 with HF7409862. This document contains important information about this release. We strongly recommend that you read the entire document.

About this release

McAfee Endpoint Encryption for PC 6.1 Patch 3 with HF7409862 provides full disk encryption and data protection for PCs and laptops. It prevents the loss of sensitive data, especially from lost or stolen equipment. It protects the data with strong access control using Pre-Boot Authentication (PBA) and a powerful encryption engine. EEPC 6.1 Patch 3 with HF7409862 is the encryption software installed on client systems. It is deployed and managed through the ePolicy Orchestrator using policies. A policy is a set of rules that determines how encryption functions on the user's computer.

This release is a repost of McAfee Endpoint Encryption for PC 6.1 Patch 3 including the changes introduced with HF7409862. The cryptographic modules contained within this release are currently undergoing FIPS certification. For more details and status updates, refer to the KnowledgeBase article https://kc.mcafee.com/corporate/index?page=content&id=KB74396.

> **NOTE:** Before you begin, make sure that you remove any competitor's encryption products from your system. Also, do not install any other encryption products after installing EEPC.

This release supports new installations, migrating your EEPC 5.x.x installed systems and upgrading EEPC 6.x installed systems to EEPC 6.1 Patch 3 with HF7409862. For more details and procedures on migrating your EEPC 5.x.x installed systems to EEPC 6.1 Patch 3 with HF7409862, see the *McAfee Endpoint Encryption for PC 6.1 Patch 2 Migration Guide*. The migration procedure used for EEPC 6.1 Patch 3 with HF7409862 is the same as the migration procedure used for EEPC 6.1 Patch 2.

- In this Release Notes, EEPC 5.x.x refers to EEPC 5.1.7 and later versions
- EEPC 6.x refers to EEPC 6.0, 6.0 Patch 1, 6.0 Patch 2, 6.1, 6.1 Patch 1, 6.1 Patch 2 and 6.1 Patch 3.

Upgrade is defined as installing a patch or major release from the same product family. In this example, it means upgrading to EEPC v6.1 Patch 3 HF7409862 from a previous EEPC v6.x release.

- Migration is defined as moving from the legacy EEPC to ePO managed EEPC. In this example, it means migrating from EEPC v5.x.x to EEPC v6.x.

> **NOTE:** For any best practices and recommendations around migration and upgrade, refer to the *McAfee Endpoint Encryption for PC 6.1 Patch 2 Migration Guide* and *McAfee Endpoint Encryption for PC 6.1 Patch 2 Best Practice Guide*. These documents also apply to EEPC 6.1 Patch 3 and EEPC 6.1 Patch 3 with HF7409862.

EEPC 6.1 Patch 3 with HF7409862 features

McAfee is committed to providing superior encryption across a variety of environments. McAfee Endpoint Encryption for PC delivers a powerful encryption solution with a strong and unique PBA that protects data from unauthorized access, loss, and exposure.

- EEPC 6.1 Patch 3 with HF7409862 is a patch release, which is an improved version of EEPC 6.1 Patch 3.
- This release supports the use of the Setec smartcard for user log on. For more details, refer to the KnowledgeBase article https://kc.mcafee.com/corporate/index?page=content&id=KB71555.
- This release is able to co-exist with the IBM Tivoli DPRA Credential Provider. For more details, refer to the KnowledgeBase article https://kc.mcafee.com/corporate/index?page=content&id=KB74394.
- The CardOS 4.4 card is supported in this release. For more details, refer to the KnowledgeBase article https://kc.mcafee.com/corporate/index?page=content&id=KB71555.

Requirements

This section provides the requirements for the McAfee ePO server and EEPC 6.1 Patch 3 with HF7409862 client.

System requirements

Systems	Requirements
ePO server systems	See the ePolicy Orchestrator product documentation for versions 4.5 and 4.6
Client systems	• **CPU**: Pentium III 1GHz or higher • **RAM**: 256 MB minimum (1 GB recommended) • **Hard Disk**: 200 MB minimum free disk space

Software requirements

Software	Requirements
McAfee management software	• ePolicy Orchestrator 4.5 Patch 4 Hotfix 1 and later • McAfee Agent for Windows 4.5 Patch 1 or later
Endpoint Encryption for PC software	• Extensions **NOTE:** EEPC 6.1 Patch 3 with HF7409862 is managed by the

	same extensions as 6.1 Patch 2. • EEADMIN.ZIP (6.1 Patch 2) • EEPC.ZIP (6.1 Patch 2) • EEPC software package • MfeEEPC.ZIP (6.1 Patch 3 with HF7409862) • EE Agent • MfeEEAgent.ZIP (6.1 Patch 3 with HF7409862)
Microsoft Windows Installer 3.0 Redistributable package (for ePO)	See the ePolicy Orchestrator product documentation for versions 4.5 and 4.6
Microsoft .NET Framework 2.0 Redistributable package (for ePO)	See the ePolicy Orchestrator product documentation for versions 4.5 and 4.6
Microsoft MSXML 6 (for ePO)	See the ePolicy Orchestrator product documentation for versions 4.5 and 4.6

Operating system requirements

Systems	Software
McAfee ePO server Systems	See the ePolicy Orchestrator product documentation for versions 4.5 and 4.6
Client systems	• Windows Server 2003 SP1 or later (32-bit only) • Windows Server 2008 (32-and 64-bit) • Windows XP Professional SP3 (32-bit only) • Windows Vista (32-and 64-bit) • Windows 7 (32-and 64-bit), (Not XP Mode)

Known issues

For McAfee Endpoint Encryption for PC 6.1 Patch 3 with HF7409862 Known Issues, refer to the KnowledgeBase article https://kc.mcafee.com/corporate/index?page=content&id=KB73391.

Resolved issues

Issues from previous releases of EEPC that have been fixed in EEPC 6.1 Patch 3 release are listed as follows:

- Some systems with AMD chips display the error message **McAfee Endpoint Encryption Fatal Error [0xEE0200006] Getting disk info**. **(BZ 649912)**
- Some localized messages are truncated in the EEPC Status window. **(BZ 681024)**

- Error writing to disk sector. **(BZ 689111, BZ 699440, BZ 709908, BZ 714993 BZ 718394)**
- Operating system does not load on Dell E6420 computers in RAID ON mode. **(BZ 689283)**
- Support for the Alcor smartcard reader is required. **(BZ 695037)**
- Endpoint Encryption Credential Provider, on a remote desktop, causes **Windows Logon issues (hanging)** at the log on screen on Windows 7 64-bit. **(BZ 695676)**
- On Pre-Boot window, the track point does not work on several Lenovo models. **(BZ 704555)**
- Internal smartcard readers do not work on Dell E4200, E6420, E6510 and M4500. **(BZ 709021, BZ 705076, BZ 705075, BZ 707900, BZ 705941, BZ 707277)**

Issues from previous releases of EEPC that have been fixed in EEPC 6.1 Patch 3 with HF7409862 release are listed as follows:

- When a USB device containing multiple device descriptors is connected the Pre-Boot environment will hang. **(BZ 718581)**
- Error reading disk sector 0xE0020007 when accessing the disk in the Pre-Boot environment on Panasonic CF-J10, CF-N10, CF-52, CF-53, HP 2760P, Elitebook 6460P, and Clevo D400S. **(BZ 714142)**
- The Pre-Boot Authentication will freeze on a Dell Latitude E5420 when the laptop is on AC power. **(BZ 734200)**
- After Pre-Boot Authentication, the Windows 7 boot process reverts to the Windows Repair menu on Sony Vaio Z, Toshiba Tecra A11, M11, Satellite L730 and Portege R830 laptops. **(BZ 738280)**
- After upgrading from EEPC 6.0, 6.0 Patch 1, 6.0 Patch 2, 6.1, and 6.1 Patch 1, the Pre-Boot environment hangs at Pre-Boot Authentication. **(BZ 740986)**

Documentation

This release of EEPC 6.1 Patch 3 with HF7409862 includes the following documentation set.

Standard product documentation

McAfee documentation provides the information you need during each phase of product implementation, from installing a new product to maintaining existing ones. This release of EEPC 6.1 Patch 3 with HF7409862 includes the following documents:

- *McAfee Endpoint Encryption for PC 6.1 Patch 3 with HF7409862 Release Notes*
- *McAfee Endpoint Encryption for PC 6.1 Patch 2 Product Guide*
- *McAfee Endpoint Encryption for PC 6.1 Patch 2 Migration Guide*
- *McAfee Endpoint Encryption for PC 6.1 Patch 2 Best Practice Guide*
- *McAfee Endpoint Encryption for PC 6.1 Patch 2 Quick Start Guide*
- *McAfee Endpoint Encryption for PC 6.1 Patch 2 Scripting Guide*

NOTE: The documentation from 6.1 Patch 2 is applicable to 6.1 Patch 3 and 6.1 Patch 3 HF7409862.

KnowledgeBase articles for EEPC 6.1 Patch 3 with HF7409862

- McAfee Endpoint Encryption versions 5 and 6 Comparison Guide (FAQ) : https://kc.mcafee.com/corporate/index?page=content&id=KB66700
- McAfee Endpoint Encryption for PC version 6.x Error Messages: https://kc.mcafee.com/corporate/index?page=content&id=KB67358
- McAfee Endpoint Encryption for PC — Supported Platforms: https://kc.mcafee.com/corporate/index?page=content&id=KB68053

- Read this before installing EEPC: https://kc.mcafee.com/corporate/index?page=content&id=KB68411
- Changes to the Endpoint Encryption Status tray dialog messages and MfeEpe.log messages between EEPC 6.1/6.1 Patch 1 and 6.1 Patch 2: https://kc.mcafee.com/corporate/index?page=content&id=KB72865
- How to load the Setec Access Token for use with Endpoint Encryption for PC 6.1 Patch 3 and 6.1 Patch 3 with HF7409862: https://kc.mcafee.com/corporate/index?page=content&id=KB73255

Supported Tokens and Readers

McAfee Endpoint Encryption for PC supports different logon tokens and token readers. The token type associated with a user or a user group can be modified using ePolicy Orchestrator. For details on modifying tokens, refer to the *McAfee Endpoint Encryption for PC 6.1 Patch 2 Product Guide*.

KnowledgeBase articles for tokens and readers in EEPC 6.1 Patch 3 with HF7409862

For more information about the supported tokens, readers and their known issues, refer to these KnowledgeBase articles:

- McAfee Endpoint Encryption for PC 6.1 Patch 3 Known Issues (Tokens and Readers): https://kc.mcafee.com/corporate/index?page=content&id=KB73391
- Supported Readers used for authentication in McAfee Endpoint Encryption for PC 6.x: https://kc.mcafee.com/corporate/index?page=content&id=KB71554
- Supported Tokens used for authentication in McAfee Endpoint Encryption for PC 6.x: https://kc.mcafee.com/corporate/index?page=content&id=KB71555
- How to use a Stored Value token in McAfee Endpoint Encryption for PC 6.x: https://kc.mcafee.com/corporate/index?page=content&id=KB71556
- How to use a PKI token in McAfee Endpoint Encryption for PC 6.x: https://kc.mcafee.com/corporate/index?page=content&id=KB71557
- How to use a Self-Initializing token in McAfee Endpoint Encryption for PC 6.x: https://kc.mcafee.com/corporate/index?page=content&id=KB71558

Before installing EEPC 6.1 Patch 3 with HF7409862

Make sure that you read this section completely and take the following precautions before installing EEPC 6.1 Patch 3 with HF7409862 on the client.

Hard Disk hardware failure during Encryption

We recommend running a CHKDSK /r prior to installing EEPC to ensure the hard disk is in a healthy state. If the Hard Disk is damaged or has a high number of undiscovered bad sectors, the disk could fail during the full disk encryption process.

In addition, McAfee recommends using Endpoint Encryption GO to discover potential issues prior to installation. For more details, please refer to the KnowledgeBase article https://kc.mcafee.com/corporate/index?page=content&id=KB72777.

Dynamic and RAID disks in Windows

Endpoint Encryption works at sector level, consequently it does not support software-based dynamic disks and software based RAID.

- **Hardware RAID**
  Endpoint Encryption is untested in this mode, but may work properly in a situation where pure Hardware RAID has been implemented. However, Endpoint Encryption cannot support diagnostic or disaster recovery in this situation.

HP NoteBook PCs with SATA hard disks

McAfee and HP discovered an issue with the BIOS support of SATA hard disks on HP Notebooks, which makes writing to the hard disk in SATA Native mode unreliable. The issue has been confirmed on the HP Compaq nw8440 Mobile Workstation, HP Compaq nc8430 Notebook PC, and HP Compaq nx8420 Notebook PC.

If SATA Native Mode is enabled on these systems, the following issues eventually occur due to incorrect writing of data by the HP BIOS:

- Corrupt pre-boot graphics and text, missing users, missing tokens
- **Data Store Corrupt** errors
- **Missing Attribute** errors
- **Unknown User** where the user previously functioned and has not been removed.

This issue is present in BIOS versions prior to F.10, released 17th April 2007. In these releases to prevent this issue occurring, please disable SATA Native Mode in your notebooks BIOS. You can obtain BIOS version F.10 and greater through your HP support service. If you are using a BIOS version of F.10 or greater then this issue is not relevant. Download the drivers and software from http://h20000.www2.hp.com/bizsupport/TechSupport/DriverDownload.jsp?prodNameId=1839208&lang=en&cc=us&taskId=135&prodClassId=-1&prodTypeId=321957&prodSeriesId=1839152

Time and date synchronization

Make sure that all laptops and systems managed by the McAfee ePO server have an accurate time and date.

General recommendations

- If you are using customized themes with EEPC 6.x, then recreate your custom themes from EEPC 6.1 Patch 3 with HF7409862 default theme after upgrade. This will ensure that the correct user interface is displayed. Failure to do so will continue to display the EEPC 6.x user interface.

  NOTE: The size limit of the PNG file that can be uploaded is 2.5 MB.

- If you are using Policy Assignment Rules to assign specific Endpoint Encryption User Based Policies (UBP) to users, then refer to the *McAfee Endpoint Encryption for PC 6.1 Patch 2 Product Guide* to learn how to configure these users to continue to use Policy Assignment Rules in EEPC 6.1 Patch 3 with HF7409862. This must be done prior to deploying the Endpoint Encryption (EE) Agent/PC to the clients. Failing to configure users correctly will result in users returning to use the default User Based Policy assigned at system level.
- After upgrading from 6.0.x to EEPC 6.1 Patch 3 with HF7409862, please run the EE LDAP Synchronization task before deploying the EE Agent/PC to the clients. EEPC 6.1 Patch 3 with HF7409862 requires additional data to be requested from the LDAP server for users that have been configured for User Based Policy enforcement.

COPYRIGHT

Copyright © 2012 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.